

Fort Drum
Classified/Unclassified Installation Campus Area network (ICAN)
Acceptable Use Policy
(AUP)
(February 2010)

The Department of Defense and the Department of the Army, specifically, AR 25-2, requires that all users must sign an AUP before being granted access to any Army Information System. In addition, failure to sign or abide by the AUP is grounds for denial or termination of access to Army Information Systems and willful violation of the terms of the AUP are potential grounds for punitive actions under the provisions of AR 25-2. For ease of understanding the AUP is subdivided into a number of sections each addressing a specific requirement or subject area. Personnel are cautioned to carefully read each section since their behavior is bound and governed by all portions of this policy.

Purpose:

This document sets forth the expected Rules of Behavior and the Acceptable Use Policy for all users of systems connected to the Fort Drum Unclassified and Classified Installation Campus Area Networks (ICANs), Virtual Private Network (VPN) remote access capabilities, Outlook Web Access (OWA) electronic mail, network or enterprise services, and all other Information Systems configured and managed by the Network Enterprise Center (NEC) Fort Drum NY.

Basic Agreement:

As an Information Systems (IS) user at Fort Drum New York, I will adhere to all security rules prescribed in this document.

References

Department of Defense Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003
DoD Regulation 5400.11-R, subject Department of Defense Privacy Program, 14 May 2007
Memorandum, Department of Defense, 18 August 2006, Subject DoD Guidance on Protecting Personally Identifiable Information
Memorandum, Office of the Secretary of Defense, 21 September 2007, Subject Safeguarding Against and Responding to the Breach of Personally Identifiable Information
AR 25-1 Army Knowledge Management and Information Technology, 4 December 2008
AR 25-2 Information Assurance, 24 October 2007
AR 340-21, The Army Privacy Program, 5 July 1985
AR 380-5 Department of the Army Information Security Program, 29 September 2000

DOD STANDARD MANDATORY NOTICE AND CONSENT

By signing this document, you acknowledge and consent that when you access Department of Defense (DOD) information systems

- 1 You are accessing a U S Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U S Government authorized use only.
- 2 You consent to the following conditions:
 - a The U S Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI).

investigations

b At any time, the U S Government may inspect and seize data stored on this information system

c Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U S Government-authorized purpose

d This information system includes security measures (e g , authentication and access controls) to protect U S Government interests not for your personal benefit or privacy

e Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants Under these circumstances, such communications and work product are private and confidential, as further explained below

(1) Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U S Government actions for purposes of network administration, operation, protection, or defense, or for communications security This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality

(2) The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation) However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies

(3) Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DOD policy Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality

(4) Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DOD policy

(5) A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy However, in such cases the U S Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality

(6) These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential Further, the U S Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected

f In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (Le , for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U S Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U S Government's otherwise-authorized use or disclosure of such information

g All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner") When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these

conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement

Army Standard Acceptable Use Policy (AUP)

As a user of an Information System (IS), I will adhere to the following security rules:

1 I know that the use and access to DOD information systems is a revocable privilege. I understand that AR 25-2 is punitive in nature and that violation of those paragraphs identified in AR 25-2, para 1-1(j), page 2 may be punished as violations of a lawful general order under Article 92 of the Uniformed Code of Military Justice (UCMJ) or under other disciplinary, administrative, or contractual actions as applicable.

2 I understand that failure to follow acceptable use and best practices jeopardizes the security of the information, the IS, the network, the Army, and DOD, and may cause irreparable harm, loss of critical information, or risk soldiers' lives and I will only use the system for "Official Use" and "Authorized Purposes." I will use Army information systems (computers, systems, and networks) only for authorized purposes.

3 I have completed the user security-awareness training. I will participate in all training programs as required, inclusive of threat identification, physical security requirements, acceptable use policies, remote access standards, and malicious content and logic identification, and incident reporting. I will become cognizant of non-standard threats such as social engineering, phishing, SPAM, and other emerging threats.

4 I acknowledge that certain activities are never authorized on Army networks. These activities include personal use of government resources involving pornography or obscene material (adult or child), copyright infringement (such as the sharing of copyright material by means of peer-to-peer software), gambling, the transmission of chain letters, use of systems for personal financial gain, unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use, or the violation of any statute or regulation. I am prohibited from unauthorized accessing, storing, or transmitting prohibited content for example pornography, chain-mail, bogus threats, copyright protected, etc.) I will not forward chain email, or distribute virus warnings. I will report chain e-mail or virus warnings to my IASO and delete the message. I will not attempt to run sniffer or other hacker-related software on the system.

5 I will take no actions that alter the security configurations or disable Information Assurance (IA) security safeguards or circumvent the security mechanisms of the IS. I will not attempt to access or modify data, crack or change passwords, or use operating systems or programs, except as specifically authorized.

6 I will not download, intentionally install or use unauthorized or malicious code, backdoors, purge tools, password crackers, or file-sharing software (including MP3 music and video files), peer-to-peer (P2P) software or games onto my Government computer, Government IT system, or network. I will not install any software or hardware to any computer or connect or relocate any device (e.g., a client, or workstation, server, Removable or Fixed Storage Media, printer, switch, hub, or wireless devices) to any Army network or Information System without prior written approval of the Fort Drum Installation Information Assurance Manager (IIAM), NEC Director, or Fort Drum Designated Approving Authority (DAA).

7 I will meet and maintain required security investigations, clearances, authorizations, and mission requirements, and appropriately be granted access to authorized information and services.

8 I know what constitutes a security incident. If I observe anything that indicates inadequate security for this system, I will immediately report it to the IASO. I will comply with security guidance issued by my SA or IASO. I will follow procedures to report security violations and incidents, abnormal behavior, system or application errors, suspicious activity, chain e-mails, spam, virus warnings, missing equipment, or the presence of unknown installed programs in accordance with local policy. I will immediately report any discrepancies in system operations following any anti-virus definition update, protective security application configuration, system update or failures.

9 I have been issued a CAC or another identifier and authenticator (user ID/password) to authenticate my access to government resources or computer accounts. After receiving them:

a I will not allow anyone else to have or use my authenticator. I am responsible for all actions conducted under my account. As the only authorized user of this account, I will protect the account(s), the authenticator(s), and all information from disclosure and will use any local or remote access privileges granted to me to perform authorized tasks or mission related functions. I will apply these same security standards when accessing or processing any information as granted through remote access using a government-provided or personal-owned system. I am responsible for all activity that occurs under that identifier while I am logged on. I will protect the PIN.

and/or password that authenticates the identifier

- b If I am assigned an individual user account I will not permit anyone else to use the account assigned me
 - c I will never reveal my individual PIN and/or password to anyone, except to authorized NEC support personnel for troubleshooting purposes only I understand that I will receive a new password after the troubleshooting has been accomplished If my account is to a classified network, I will protect the password at the highest classification level of the network
 - d If technically capable of doing so, I will immediately change the individual password issued to me on my first log-in - regularly thereafter as directed I will ensure my password meets current Fort Drum and Army directives (e g , length, character set, no prohibited sequences or combinations)
 - e I will not store my CAC PIN or password on any connecting device or on any magnetic or electronic media
 - f I will never leave my computer unattended and logged-on, unless secured by an appropriately PIN/password protected screen saver set to activate after 3-5 minutes of inactivity
 - g I will always remove my CAC from the computer system when departing my work area, even if only for brief periods of time
 - h I will log off my computer system at the end of my duty day
 - i I know it is a violation of policy for any user to seek to mask or hide their identity, or to seek to assume the identity of another
 - j If my account is on a classified network, I understand that my authenticator is classified at the highest level of information on that network, and I will protect it in the same manner as that information I will change my authenticators to meet existing policies
 - k If I am a member of a group account, I am responsible for all activity when I am logged on a system with that account
- 10 I understand there are many more procedures, official regulations and policies applicable to information-system operations, and this certificate is only a short summary to stress key points

Handling Media and Output

- 1 I will properly mark all electronic correspondence where it applies in accordance with AR 380-5 Chapter 4, and AR 380-19 I will properly mark, encrypt, and control output and removable media while I am using any system to include printed materials in accordance with AR 380-5 and AR 25-2
- 2 I will check all storage media for malicious software and scan for viruses before loading on any system

Training

I understand that the DoD and Department of the Army have mandated initial and recurring training on a variety of topics related to use and protection of Information Systems and Sensitive Information Specifically, I understand that

- 1 I must complete initial Information Assurance (IA) Awareness training before I can obtain access to any classified or unclassified Information Systems at Fort Drum
- 2 I must complete IA Awareness refresher training annually
- 3 I must complete training on protection of Personally Identifiable Information (PII) on an annual basis
- 4 I must complete any additional training as directed by the DoD, Army, or NEC
- 5 I will establish an account on the Army Training and Certification Tracking System (ATCTS) to ensure my training is properly entered and tracked <https://atc.us.army.mil/iastar/>
- 6 I realize that failure to complete all prescribed training is grounds for termination of access to all Fort Drum Information Systems

Classified Information Systems

If connected to the Army SECRET Internet Protocol Router Network (SIPRNET) or working on a stand-alone classified system I know

- 1 My system operates at least in the US SECRET, "system high" mode of operation for SIPRNET and at the highest classification level for the information processed on the stand-alone system
- 2 All media, devices, and output from classified systems must be marked and handled IAW AR 380-5
- 3 Any storage media used on the system immediately becomes classified and protected at the system-high level, regardless of the implied classification of any data contained on it (until declassified or downgraded by an approved process)
- 4 I must protect all printed output at the system high level until I, or someone with the requisite clearance personally reviews it and classifies (grades) it appropriate to actual content
- 5 I will not enter information into the system if the information is of higher classification level than the system I will not enter information that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved in writing by the Fort Drum Designated Approving Authority (DAA), NEC Director, or Fort Drum Installation Information Assurance Manager (IIAM)
- 6 Only U S cleared personnel with a verified "need to know" are allowed unescorted access to the system
- 7 Storage media may not be removed from the computer area without local commander approval
- 8 If I must transport classified material I will have in my possession a valid Fort Drum Courier Card, DD Form 2501 and all classified material will be packaged IAW AR 380-5
- 9 I understand the classification boundary between classified and unclassified networks and systems requires vigilance, and that Foreign Nationals and personnel without a current clearances and valid "need to know" are not permitted to view screens connected to the SIPRNET or operated in a stand-alone mode

Telework and Remote Connection Rules

If I perform Telework or use the NEC provided Virtual Private Network (VPN)

- 1 I understand that any government computer being used for telework or remote access must employ the NEC-provided Virtual Private Network (VPN) client and must connect through and authenticate with the Fort Drum Domain Under no circumstances should a government provided computer be connected to a commercial Internet Service Provider (ISP) without using the VPN
- 2 I understand that any government computer being used for telework or remote access must employ data encryption to protect Sensitive Information on the hard disk The system must employ the NEC configured Microsoft Windows Encrypted Files System (EFS) for protection of all sensitive data

Network Access

- 1 I will not connect any equipment to the Fort Drum ICANs without prior written approval from the Fort Drum Designated Approving Authority (DAA), NEC Director, or Fort Drum Installation Information Assurance Manager (IIAM)
- 2 I will NOT alter any network drops on Fort Drum
- 3 I know that, to the greatest extent possible, network cables will not be extended beyond a distance which can be constantly observed by the user
- 4 I know that, while in garrison, systems will only be connected to authorized, NEC-provided network drops and equipment
- 5 I will always logon to and authenticate through the Fort Drum domain, unless performing off-line processing where no network connection is available
- 6 At no time will I access the Internet on a government Information System without first authenticating through the Fort Drum domain or obtaining prior written approval from the Fort Drum Designated Approving Authority

Handling and Protecting Sensitive Information (SI) And Personally Identifiable Information (PII)

Sensitive information is defined as: Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 USC 552a (The Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive information includes information in routine DOD payroll, finance, logistics, and personnel management systems. Examples of sensitive information include, but are not limited to, the following categories:

- FOUO, in accordance with DOD 5400 7-R, is information that may be withheld from mandatory public disclosure under the FOIA
- Privacy data is personal and private information (for example, individual medical information, home address and telephone number, social security number) as defined in the Privacy Act of 1974. This is referred to as Personally Identifiable Information (PII)

1 I understand that ALL Sensitive Information must be protected from unauthorized disclosure and that I will do so by utilizing the encrypted file folder provided for me on my government provided computer

2 I also understand that any loss of Sensitive Information must be immediately reported to my Chain-of-Command IAW the Fort Drum Policy Memorandum, 09-15, Personally Identifiable Information

Use of Employee Owned Information Systems (EOIS)

Employee-owned information systems (EOISs), media devices, Personal Electronic Devices (PEDs), Mobile Computing Devices (MCDs), or related technologies are prohibited for any classified use, and should be prohibited for sensitive information access or processing or operating in areas where this processing occurs. EOISs, MCD, and PEDs must be authorized/registered with command security personnel when carried into restricted or secure areas and the required control measures have been verified.

1 I know the use of employee-owned information systems (EOIS) is prohibited for storing, processing or transmitting classified or Sensitive Information

2 I know that any use of an EOIS for ad-hoc (one-time or infrequent) processing of unclassified, publically releasable information is restricted and must have prior approval from the Fort Drum Designated Approving Authority (DAA), NEC Director, or Fort Drum Installation Information Assurance Manager (IIAM)

3 I understand that any employee owned information system (EOIS) used for ad hoc performance of official duties, to include checking Outlook electronic mail via the web (OWA), must have a Department of the Army approved anti-virus application loaded and configured for constant virus detection

4 I know that, that if approved for ad hoc use, EOISs processing official data will comply with all security provisions of AR 25-2. Computer owners will implement Information Assurance (IA) countermeasures required by AR 25-2, specifically AV and IA software and updates, or be prohibited from remote access. If data is temporarily stored on an approved EOIS, it must be deleted at the end of that day's work session. All processed or stored data will be removed from the EOIS and personnel will sign compliance statements that the data was removed.

5 I will scan all data processed from an EOIS before inclusion or introduction into the network or any government IS

6 I will NOT perform any remote access for remote management from an EOIS

Once you have read and understand all requirements listed above fill out the identification blocks below, sign (either digitally or manually), then save and upload the document (in PDF format) to the Army Training & Certification Tracking System (ATCTS) at the following web site: <https://atc.us.army.mil/iastar/>

Rank/Full Name:

Organization:

DSN:

E-Mail:

Acknowledgement:

I have read the above requirements regarding use of DOD information systems. I understand there are many more procedures, official regulations, and policies applicable to information-system operations, and the above is only a short summary to stress key points. I understand my responsibilities regarding these systems and the information contained herein and that failure to abide by the rules could result in revocation of my user privileges and network access and that punitive or administrative disciplinary action could be taken against me. My signature below constitutes my acknowledgement of and agreement to abide by these rules.

Sign or Insert Digital Signature in the block below:

IASO/Security Manager Certification: The user named above meets all training and clearance requirements for network access.

IASO
Name/Rank/Signature

Date:

Security Manager
Name/Rank/Signature

Date: